Deirdre Menard
CEO
LucidTech LLC
1030 15th Street, NW, Suite 1400
Washington, DC 20005
Phone 202.650.0409
dmenard@lucidtech.digital

June 20, 2019

Ex Parte
Via ECFS

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: ***Advanced Methods to Target and Eliminate Unlawful Robocalls,*** CG Docket No. 17-59
and
Call Authentication Trust Anchor, CG Docket No. 17-97

Dear Ms. Dortch:

On June 20, 2019, I met with Mark Stone, Deputy Bureau Chief, Kurt Schroeder, Chief of the Consumer Policy Division, Kristi Thornton, Acting Deputy Consumer Policy Division Chief, and Jerusha Burnett, Consumer Policy Division Attorney Advisor. As representative for LucidTech, I voiced our continued support for the Commission's ongoing efforts to address malicious and harassing robocalls, and our appreciation for its recognition of the importance of restoring trust in voice calls.

We discussed LucidTech's commitment to the elimination of unlawful and nuisance robocalls, as well as LucidTech's role in creating solutions to address the problem to date. LucidTech shared its position regarding the necessary steps required to support tracebacks in an effective and timely manner as SHAKEN/STIR is deployed.

We also discussed LucidTech's position regarding the challenges associated with a verification display intended to demonstrate to the public that the call has been attested to via SHAKEN/STIR. SHAKEN/STIR attests to the authenticity of the telephone number being displayed on the screen as being that of the caller, versus a spoofed telephone number. However,

because the intent of calls cannot be attested to and because callers with fraudulent intent will be able to make outbound phone calls from telephone numbers which have legitimately been assigned to them, we suggest it is possible that providing a green checkmark or other verification display runs the risk of conferring validity to the phone call beyond the display's intent. For this reason, we suggested that it is possible that SHAKEN/STIR provides the most value behind the scenes, informing service providers' robocall analytics, rather than as an additional piece of on-screen information for consumers to decipher. We addressed similar challenges relating to the display of Rich Call Data or Rich Calling Display (aka RCD), and the ongoing maintenance required to keep information current. We also discussed the related challenges involved in allowing entities to self-identify which caller category should be displayed when their calls are received.

LucidTech shared with members of the FCC our position that SHAKEN/STIR enables a more robust traceback model, and that tracebacks must evolve to be automated, secure, and provide real-time, data-driven reporting. Related to the information this reporting would provide, LucidTech suggested that now is the time to consider what mechanism may be employed to address providers who routinely allow bad traffic onto the network. Also related was our suggestion that robocall analytics providers ensure that their dispute resolution process is as automated as possible, in order to allow enterprise and consumer telephone service customers to address any perceived mischaracterizations of their calls as spam or scam.

LucidTech raised the question of international cooperation with respect to robocall mitigation, and suggested that it is time to look for international cooperation and collaboration opportunities in order to move this next phase forward.

Finally, we discussed our perceived need for an ongoing bridge between policy and technology groups within various organizations as the technology around robocall detection and mitigation is rolled out and evolves.

Pursuant to Section 1.1206(b)(1) of the Commission's rules, I am submitting this *ex parte* notice letter into the above-referenced docket over the Electronic Comment Filing System.

Sincerely,

/s/

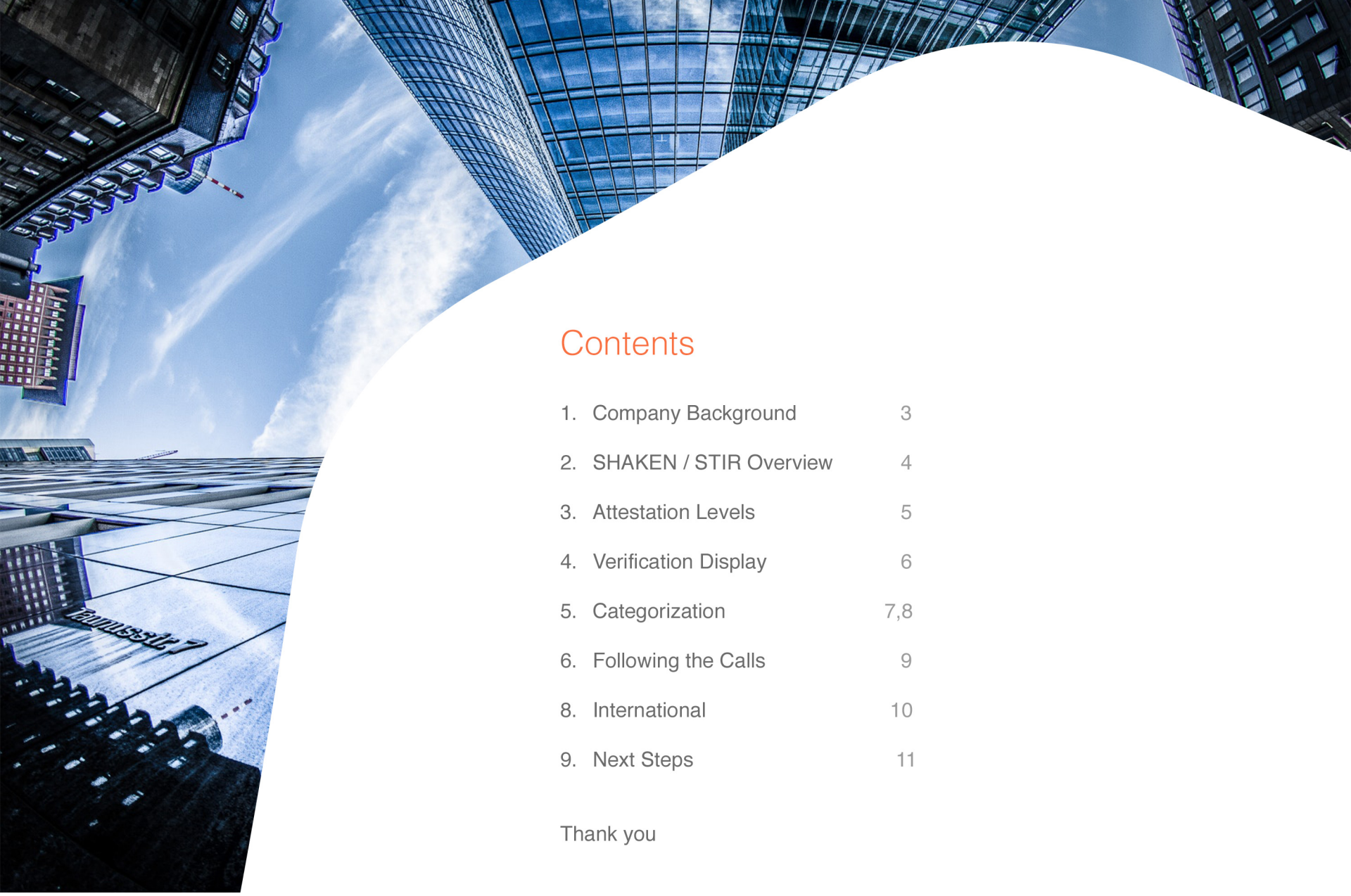
Deirdre Menard
CEO, LucidTech LLC

Robocalling 2019

SHAKEN / STIR and beyond

presented to members of the FCC
June 20, 2019

LUCIDTECH



Contents

Thank you

LUCIDTECH

Company Background

LucidTech is a solution provider to the tech industry with deep knowledge of and a longterm focus on the robocall problem.

In early 2016, LucidTech began work with Transaction Network Services (TNS / Cequint) to launch their Call Guardian robocall mitigation service.

LucidTech provided product, project, and strategy solutions, RFP & NPRM response services, and represented TNS in industry and policy discussions.

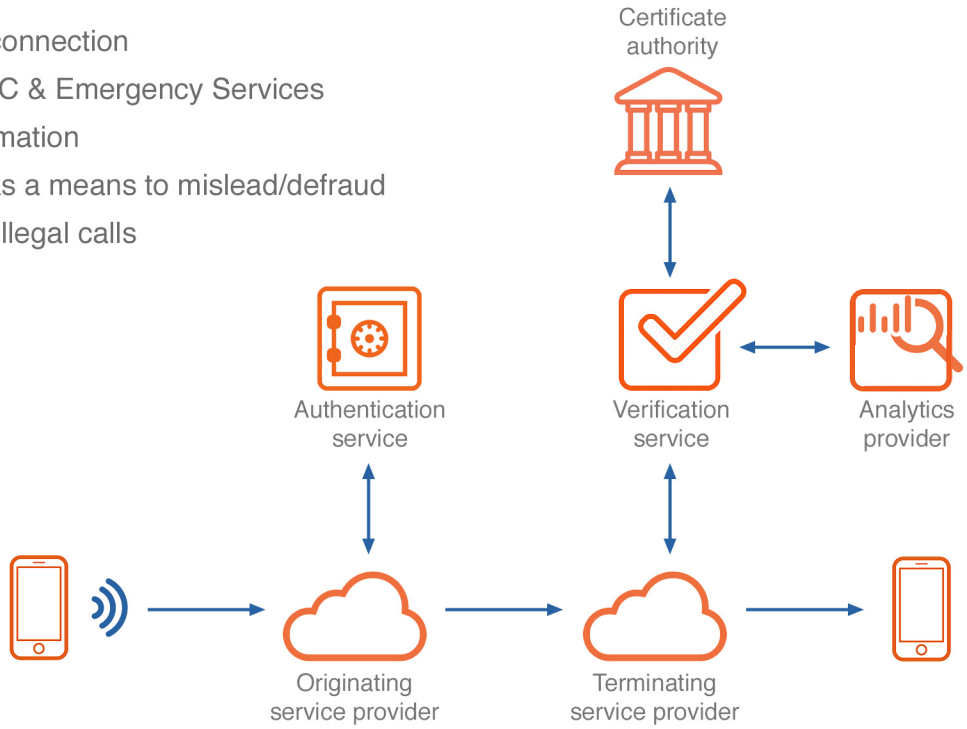
LucidTech now works with a range of clients in the robocall space, advising them with solutions and strategies, and participates in industry forums and ongoing discussions about restoring trust in voice calling.

For more information, please visit www.lucidtech.digital or follow us on LinkedIn, Twitter, and Facebook.

LUCIDTECH

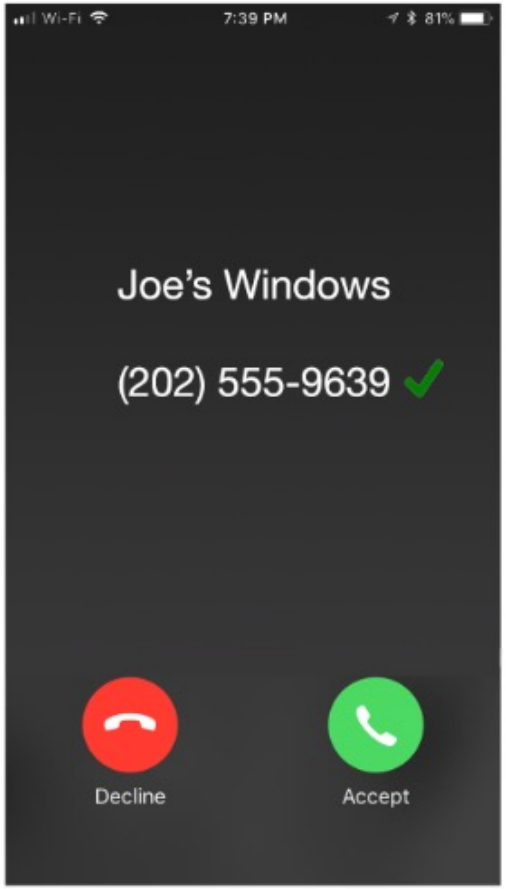
SHAKEN / STIR Overview

- Does not attest to intent of caller
- Requires uninterrupted SIP to SIP connection
- Provides levels of attestation: A, B, C & Emergency Services
- Does not block calls; provides information
- Intended to address spoofed calls as a means to mislead/defraud
- Provides mechanism to trace back illegal calls



LUCIDTECH

Attestation



A Attestation (including pre-paid SIM): The plan is for a positive indicator adjacent to the telephone number.

"This is my customer and I can attest fully to the authenticity of the number."

B Attestation (includes PBX today, but a mechanism to provide A-level is being explored): No indicator.

"This is my customer and I can ID the customer but am not saying anything about the number."

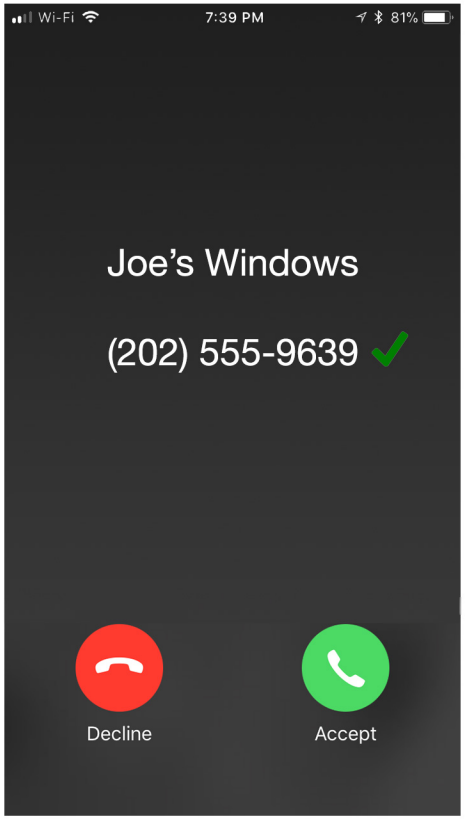
C Attestation (gateway): No indicator

A negative display will only occur if indicated based on analytics.

LUCIDTECH

Verification Display

- Predict bad actors will cycle through numbers legitimately assigned to them
- Layers of information for consumers to decipher
- Education historically a challenge
- Differentiation between trusting caller and trusting number
- Service providers seek to demonstrate efforts
- Does SHAKEN / STIR work better behind the scenes?



This is the sort of display being discussed as the likely implementation among most major providers for A-level attestation.

May still be a bad actor calling from a number that they have been assigned, and may not yet be marked as posing a risk in analytics.

Checkmark only attests to the fact that this number is legitimately assigned to the caller. Would a consumer understand this?

Does this display undermine the project if it's not well understood by consumers? Could this actually confer legitimacy? What happens to project and/or service provider reputation if consumers are defrauded by callers whose calls carried a green checkmark?

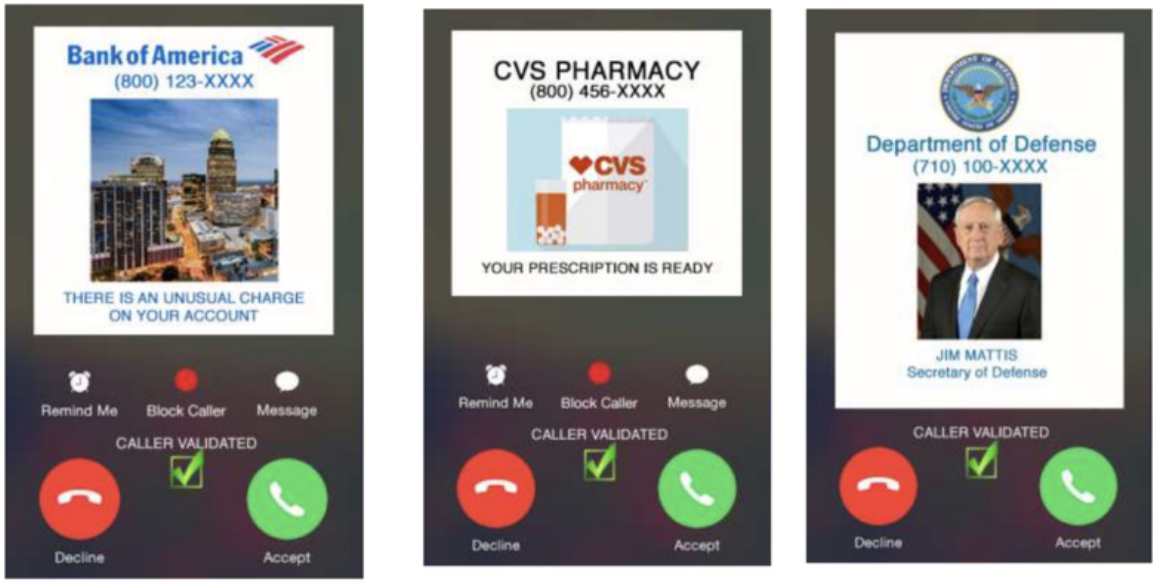
LUCIDTECH

Categorization

In theory, Rich Call Data (RCD) looks good. Smartphones being smart. And granular categories (debt collector, charity, political, pharmacy, airline) would be helpful for many reasons. However, this additional data carries the potential to increase consumer risk.

Use case: I am a service provider. I may be able to verify information provided to me, or a third-party vetting service I depend on, from a well-known large enterprise customer, but how do I trust/verify the information provided by a lesser-known entity? They will expect equal treatment and availability of services.

If that lesser-known entity's category or display of intent is approved today, what prevents them from being good at the time they were evaluated, but not so good tomorrow? Who ensures that this information remains accurate?



courtesy Richard Shockey

LUCIDTECH

Categorization

Today, analytics cannot reliably infer categorization at a granular level; instead, it must be provided by the callers. The challenges with the caller self-identification method are trust and maintenance.

Use case: I'm the calling entity. I'm legitimate in the sense that I'm not engaging in fraud. However, I want more of my calls answered than would happen if I were accurate about my intent, so I may choose a classification that is fuzzy or inaccurate in order to increase the likelihood. This could leave call recipients feeling tricked.

Alternatively, my intent is to defraud and I'm using a number I've been assigned to make my calls. Very careful checks would have to be in place to prevent a classification such as 'debt collector' that would confer legitimacy on my fraudulent demand for money. If this occurs alongside a green checkmark, which is possible, a consumer will have increased certainty that they're being contacted about a legitimate debt.

Further, a provider who, today, would assign me a number and ignore the fact that I engage in improper calling practices would likely allow me to categorize myself in any way I choose, if they're the ingress point for my self-declared information. Any mis-categorization will become the call recipient service provider's headache.

In the end, these discussions generally return to the conclusion that accurate Caller ID is of more value and easier to manage than a classification system.

Following the Calls

Along with addressing spoofing, SHAKEN / STIR facilitates tracebacks

1. To scale to support the promise of SHAKEN / STIR, traceback must be automated, secure, and data-driven. Questions about how volume tracebacks are initiated and addressed remain open. Dependencies on some mechanisms introduce risk

2. The origid, used as an origination identifier, should not be cycled through (this has been discussed, citing privacy concerns), but should be consistent

    a) The origid should be supplied consistently to Analytics Providers in order to allow them to identify patterns

3. Providers who routinely supply bad traffic must be evaluated. What recourse does SHAKEN / STIR provide? e.g., their certificates could be revoked by the STI-PA (Policy Administrator)

LUCIDTECH

International

Looking ahead, it is going to be increasingly important to extend trust to other countries.

Where do we see the greatest opportunities to collaborate? Where is the greatest need for cooperation?

Next Steps

1. Process
    a) Bridge engineering and policy

2. Analytics Providers
    a) Automate dispute resolution process from Analytics Providers to address enterprise concerns about characterization of calls
    b) Consider whether Analytics Providers also require safe harbor provisions & have rights to required customer information under CPNI rules related to fraud detection
        i. Ensure that use of that data is siloed
    c) Support analytics and traceback by maintaining a static origid

3. Commission may wish to consider its position on verification display and challenges inherent in self-categorization for RCD and/or granular categories

4. Readiness for likelihood that bad actors may move to the use of legitimate telephone numbers in reaction to SHAKEN / STIR. What recourse for those providers who allow that traffic onto the network?

5. Evaluate evolution of tracebacks

6. Begin to examine roadmap for international collaboration

LUCIDTECH

Thank You

dmenard@lucidtech.digital

www.lucidtech.digital

LUCIDTECH